Chief Information Officers Section
Office of the Governor
State of Utah

August 26, 2002

HIPAA and Related Security Requirements

Agency Common Technical Requirements

Each agency represented in the work group has submitted security requirements from federal agencies such as Health and Human Services (HIPAA), Criminal Justice/FBI (CJIS), Public Safety, Internal Revenue Service (Common Criteria and EAL3 Evaluation), and others. The scope of this project addresses technical security and incidental privacy while not directly addressing privacy or process issues. The following requirements will be used as the basis for benchmarking existing state technology and policies.

Access Control: Access control mechanisms must be employed across all State of Utah networks, as defined by paragraph 2 of the State Information Security Policy, to ensure a given user has been granted the permission to access a system, or system resource in the manner authorized pursuant to the State User Authentication Policy.

Advanced Authentication: Advanced authentication shall be used in cases where un-trusted inbound traffic (with the exception of Internet mail and push broadcasts) is accessing the authorized State of Utah network. Authentication of the unique user identity can be a unique encrypted logon and password combination and/or use of other authentication methods including but not limited to biometrics, smart cards, tokens, digital signatures (such as VeriSign), etc.

Audit Trails: For any State of Utah operated network, functionality shall be added for real-time monitoring of networked and host-based systems to detect security vulnerabilities and incidents. The time source for logging devices shall be synchronized to a common-accessible, centralized, State of Utah time source. The minimum amount of information to be captured in an audit record is:

1. The identity of each user and, where possible, the device having access to the system or attempting to access the system.

2. The time and date of every successful or unsuccessful access.

3. Any activities which might modify, bypass or negate security safeguards controlled by the computer system.

Authorization: Once authenticated, users must be granted only specific access to the system's resources that they require to perform their duties.

Encryption: To prevent unauthorized disclosure of sensitive and valuable information, all host access to restricted information to/from the state authorized network from unauthorized networks must be encrypted with no less than 128 bit encryption. File encryption must provide an equivalent level of protection. Examples of encryption mechanisms that provide 128 bit or better encryption are Secured Socket Layer (SSL), Point-to-Point Tunneling Protocol (PPTP), Advanced Encryption Standard (AES), RSA (Rivest, Shamir & Aldeman) Elliptic Curve Cryptograpy (ECC), etc.

Firewalls: Firewall deployment on the State WAN shall follow the State Firewall Policy.

Identification: The source of any access to sensitive/restricted information must be uniquely identified.

Intrusion Detection: State of Utah locations with hosts containing sensitive/restricted information must include intrusion detection systems.

Virus Protection: State of Utah locations will incorporate virus detection/protection measures that comply with the State Virus Detection Policy.

Logging: All transactions involving sensitive/restricted information under the custody of the State of Utah networks or access devices must be logged. Furthermore, all suspicious activity, which might be an indication of unauthorized usage or an attempt to compromise security measures must also be logged and reported to ITS Security. The integrity of these logs must be protected. These logs must be removed from the recording systems and stored in a physically protected container and stored for not less than 7 years. Access methods to retrieve information from the logs must be provided, and, the logs must be reviewed periodically to ensure that the security standards are being met.

Physical Security: Resources present on state authorized networks must be physically secured from unauthorized persons.

System Design Documentation: Any agency in custody of sensitive/restricted information must develop and maintain written documentation of the overall design and security features of their system. Overall design and security features must be reviewed, the implementation tested and the test results documented. In accordance with the intent of this document, results are considered sensitive/restricted information.

Vulnerability Assessment: Vulnerability checks must be conducted on the design, and periodically after implementation. Unless otherwise specified by statute or best practice, periodic testing shall occur at least every 12 months. Results of testing and vulnerability scanning must be documented.

Vulnerability Patching: State agencies are responsible for the application of fixes or measures to stop the exploitation of known vulnerabilities.

Definitions

Access: Opportunity to make use of an automated information system resource and the ability to have contact with a terminal from which a transaction may be initiated.

Access Control: Procedures and controls that limit or detect access to critical information resources. This can be accomplished through software or biometric devices or physical access to a controlled space.

Access Path: Means or methods taken to obtain access.

Advanced Encryption Standard (AES): A Federal Information Processing Standard (FIPS) that will specify a cryptographic algorithm for use by U.S. Government organizations to protect sensitive (unclassified) information. The proposed algorithm is called Rijndael pronounced “Rhine Dahl” and is considered to provide the best combination of security, performance, efficiency, ease of implementation and flexibility.

Advanced Authentication: Access management protocols (such as tokens or similar two factor authentication) employing single use, encrypted passwords for login procedures.

Audit: The independent examination of records and activities to ensure compliance with established controls, policy, and operational procedures, and to recommend any indicated changes in controls, policy, or procedures.

Audit Logging: The process of gathering and saving information in a written or automated electronic form to record the session initiation and termination messages, logins and failed login attempts, logout, file access or other various activities to include all forms of access violations such as attempts to access data beyond the level of authorized access.

Audit Trail: A chronological record of system activities that is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.

Authentication: To positively verify the identity of a user, device, or other entity in a computer system. Often as a prerequisite to allowing access to resources in a system; the proof of the unique alphanumeric identifier used to identify an authorized CJIS system user.

Authorized Network: Those networks deemed to have applied security and reliability standards that meet criteria set forth by state, federal, and private information policies.

Biometrics: Automated methods of authenticating or verifying a user based on physical or behavioral characteristics.

Demilitarized Environment: Refers to the DMZ (De-Militarized Zone) A middle ground between an organization's trusted internal network and an un-trusted, external network such as the Internet. The DMZ is a sub network (subnet) that may sit between firewalls or off one leg of a firewall. This is the environment where un-authorized services and/or networks should live. This environment is by design not secured and as such should be treated as un-authorized..

Digital Signature: A cryptographic process used to assure the authenticity and non-repudiation of a message originator and/or the integrity of a message. A seal of confidence, which enables a recipient of a message to authenticate the sender of a message and verify that the message, was intact, or modified as it was sent.

Encryption: The process of cryptographically converting plain text electronic data into a form unintelligible to anyone except the intended recipient.

Ethernet: A distributed packet switching infrastructure connecting a group of machines together by high-speed cables to form a network.

Firewalls and Firewall-type Devices: Access control mechanisms that act as barriers between two or more segments of a computer network or overall client/server architecture, used to protect internal networks or network segments from unauthorized users or processes. These mechanisms can be either hardware or software based.

Intrusion: Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource.

Intrusion Detection: Techniques**,** which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.

Intrusion Detection System (IDS): A software package that collects information from a variety of system and network sources, analyzes the information stream for signs of misuse (attacks originating within the system or network) or intrusion (attacks or attempted attacks from outside), and reports the outcome of the detection process.

Logging: The process of storing information about events that occurred on the firewall, host system, or network. This process creates audit logs.

Network: A collection of computers and other devices, which are able to communicate or interchange information with each other over a shared wiring configuration. Such components may include automated information systems, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

Non-repudiation: A method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.
Physical Security: (1) The measures used to provide physical protection of resources against deliberate and accidental threats. (2) The protection of building sites and equipment (and information and software contained therein) from theft, vandalism, natural and manmade disasters, and accidental damage.

PPTP (**Point-to-Point Tunneling Protocol):** A protocol that encapsulates other protocols for transmission over an IP network. For example, it can be used to send NetWare IPX packets over the Internet. Due to its RSA encryption, PPTP is also used to create a private network (VPN) within the public Internet. Remote users can access their corporate networks via any ISP that supports PPTP on its servers.

RSA Elliptic Curve Cryptography: A public key cryptography method that provides fast decryption and digital signature processing. ECC uses points on an elliptic curve to derive a 163-bit public key that is equivalent in strength to a 1024-bit RSA key. The public key is created by agreeing on a standard generator point in an elliptic curve group (elliptic curve mathematics is a branch of number theory) and multiplying that point by a random number (the private key). Although the starting point and public key are known, it is extremely difficult to backtrack and derive the private key.

Security Control: Hardware, programs, procedures, policies, and physical safeguards that are put in place to assure the integrity and protection of information and the means of processing it. The ability of a criminal justice agency to set, maintain, and enforce standards for the selection, supervision, and termination of personnel and policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that make up and support a telecommunications network and related CJIS systems used to process, store, or transmit criminal justice information, guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.

Sensitive/Restricted Information: Information that requires special precautions to protect it from unauthorized viewing, modification or deletion. This shall include, but not be limited to; public, private, protected, or, controlled information.

Smart Card: A card or token containing electronic memory or possibly an embedded integrated circuit (IC), used to authenticate a user. The card may contain user information, an encryption algorithm, or even an encoded image.

SSL (Secure Socket Layer): A session layer protocol that provides authentication and confidentiality to applications.

Stateful Packet Inspection: Each time a connection is established for inbound or outbound traffic flow through the firewall, the information about the connection is logged in a stateful session flow table. The table contains the source and destination addresses, and other session-specific information. This information creates a connection object in the firewall-operating environment. Thereafter, inbound and outbound packets are compared against session flows in the connection table and are permitted through the firewall only if an appropriate connection exists to validate their passage. This connection object is temporarily set up until the connection is terminated.

Token Devices: A device for authenticating a user, similar to a smart card. A token device can contain user information or an encryption algorithm.

Trusted Network: This is synonymous with authorized network.

Un-trusted Network: This is synonymous with un-authorized network.

Un-authorized Network: This applies to any network that does not adhere to state, federal, or private information policies. This includes demilitarized environments and networks.

Virus: A self-replicating, malicious program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed.

Virus Detection: A process or program that detects, identifies, and filters viruses. Virus detection software must be constantly updated to keep up with the virus variants that emerge from the wild, especially from the Internet community.

Vulnerability: A vulnerability is a weakness in an automated information system (e.g., system security procedures, hardware, design, internal controls) that could be exploited to cause harm.

References

Common Criteria for Information Technology Security Evaluation, Version 2.1, CCIMB-99-031, http://csrc.nist.gov/cc/ccv20/ccv2list.htm

Computer Desktop Encyclopedia, The Computer Language Company, Inc., Point Pleasant, PA, (n.d.) http://www.computerlanguage.com.

State of Utah, Department of Corrections; Department of Human Services, Administrative Office of the Courts; Utah State Tax Commission; Department of Work Force Services; Department of Health Security Requirements Documentation

US Internal Revenue Service, *Penalty Provisions Under The Internal Revenue Code— IRC Sec. 7213 Unauthorized Disclosure Of Information)*

US Department of Justice Federal Bureau of Investigation (*CJIS Security Policy, July 2001, V2)*

US Social Security Administration. *Information System Security Guidelines for Federal, State and Local Agencies Receiving* Electronic Information from the Social Security Administration)